PASTA Worksheet

I. Business and Security Objectives:

The application for the sneaker company will handle various business-critical processes. The key business requirements identified include:

- Secure processing of financial transactions, ensuring confidentiality and integrity.
- Compliance with industry regulations like PCI-DSS due to handling payment card data.
- Ensuring customer data privacy and meeting legal obligations such as GDPR.

II. Technical Scope:

The sneaker company's application employs the following technologies:

- Application programming interface (API)
- Public key infrastructure (PKI)
- SHA-256 hashing algorithm
- SQL databases

Prioritizing PKI and SHA-256 ensures robust encryption and secure data handling. The importance of PKI lies in authenticating users and securing communications, while SHA-256 is vital for securely hashing sensitive data such as passwords. Ensuring the security of API calls is essential to prevent unauthorized access.

III. Application Decomposition:

The sneaker company's application consists of several core components, including the frontend web interface, backend server, databases, and payment gateway. Data flows from the user's browser to the server where it is processed and stored in a secure SQL database. Transactions are handled through a secure payment gateway, which integrates via an API.

IV. Threat Analysis:

Internal Threats:

- Insider attacks: Employees with elevated privileges could misuse their access to sensitive information, leading to data breaches.
- Misconfigured database access controls could expose critical data.

External Threats:

- Phishing attacks could trick employees into granting unauthorized access.
- SQL injection: Attackers may exploit vulnerabilities in input fields to gain unauthorized access to the database.

V. Vulnerability Analysis:

- Weak authentication mechanisms in the API could allow attackers to bypass access controls.
- SQL injection vulnerabilities could lead to unauthorized data access or data loss if proper input validation and sanitization are not enforced.

VI. Attack Modeling:

An attack tree for the sneaker company's application includes:

- Root Node: Gain unauthorized access to sensitive data.
  - Sub-node 1: Exploit SQL injection vulnerability in the login page.
  - Sub-node 2: Bypass weak authentication mechanisms in the API.
  - Sub-node 3: Launch a man-in-the-middle attack to intercept communications.

VII. Risk Analysis and Impact:

To mitigate the identified risks, the following security controls can be implemented:

1. Multi-factor authentication (MFA) to secure user accounts and reduce the risk of unauthorized access.

2. Regular security patching and vulnerability scanning to ensure that known vulnerabilities are identified and addressed.

3. Implementing database encryption to protect sensitive customer data at rest.

4. Web application firewall (WAF) to prevent attacks such as SQL injection and cross-site scripting (XSS).